

REMARKS

Claims 1-10, 12-19, and 21-32 are pending. Claims 11 and 20 have been canceled, new claims 31-32 have been added, and claims 1-3, 6-8, 10, 12, 16, 18, 23-25, and 27 have been amended.

In the action mailed October 5, 2004, the drawings were objected to under 37 C.F.R. § 1.83(a) as not showing the subject matter of claim 20. Although claim 20 has been canceled, subject matter therefrom has been added to claim 18, and thus the objection is not moot.

The objection indicated that that drawings did not illustrate the receipt of secured information from a source other than the server. In light of claim 18, it is the *second access component* that is received from the source.

FIG. 5 has been added to show the receipt of the second access component from a source other than the server from which secured information has been received. The subject matter of FIG. 5 is believed to be fully supported by, e.g., page 12, line 21-26. Thus, no new matter has been added.

Claim 1

In the action mailed October 5, 2004, claim 1 was rejected under 35 U.S.C. § 102(b) as anticipated by U.S. Patent No. 5,937,066 to Gennaro et al. (hereinafter "Gennaro").

As amended, claim 1 relates to a method that includes defining a key and a set of values, sending a first but not all of the values of the set and information encrypted using the key to a server for storage, and sending a second but not all of the values of the set to a first delegate. The key is determinable by the values and a predefined relationship between the values. The encrypted information is accessible with the key,

Amendments to the Drawings

The attached "replacement" sheet of drawings includes new FIG. 5. FIG. 5 has been added to show an implementation described, e.g., at page 12, line 21-26.

Attachments following last page of this Amendment:

Replacement Sheet (1 page)

inaccessible with the first of the values absent the second of the values, and inaccessible with the second of the values absent the first of the values.

Gennaro neither describes nor suggests sending a first but not all of the values of a set of values by which the key is determinable and information encrypted using the key to a server for storage. Gennaro also fails to describe or suggest sending a second but not all of the values of the set to a first delegate.

Rather, Gennaro describes a key recovery system that allows law enforcement or other officials to recover an encryption key that is attached to the same message which it encrypts. These attached keys are themselves encrypted so that, if a message is intercepted, the interceptor does not automatically have access to the message.

In particular, Gennaro's attached keys are encrypted by 3rd party agents. See col. 6, line 26-35 of Gennaro. To allow this encryption to occur, the information for determining the keys are sent to the 3rd party agents in encrypted form, using the 3rd party agents' public key. See col. 9, line 14-22. The 3rd party agents encrypt the information and return the encrypted information to the senders of the message. See col. 9, line 20-22.

Gennaro's encrypted messages between a sender and receiver are sent with the encryption key for that message attached. Therefore, Gennaro neither describes nor suggests sending a first but not all of the values of a set and information encrypted using the key to a server for storage. In Gennaro, the entire key is sent with every message, albeit in encrypted form. There are no values by which the key is determinable that are sent with the message.

Even if one were to neglect the fact that the entire key is attached to every message it encrypts, and consider the entire encrypted key to be a value by which the key is determinable (which applicant does not concede), claim 1 would still not be anticipated by Gennaro. In particular, under this interpretation of the claim language, the 3rd parties' private keys (which decrypt the attached key) are required to be values by which the key is determinable. However, Gennaro neither describes nor suggests sending such a second value to a first delegate. The third parties in Gennaro never transmit their private keys, but rather maintain the private keys in secrecy, even after the contents of an encrypted communication are recovered. See, e.g., col. 18, lines 31-47.

Since Gennaro neither describes nor suggests elements and limitations from claim 1, claim 1 is not anticipated by Gennaro. Accordingly, applicant requests that claim 1, and the claims dependent therefrom, be allowed.

Further, claims 2-3 recite a second set of values by which a key is determinable. Gennaro describes the transmission of an encrypted message between a sender and a recipient. There is nothing in Gennaro that describes or suggests a second set of values by which the key to Gennaro's encrypted messages is determinable. Rather, in the context of transmitting a message between a sender and a recipient, multiple sets of such values would seem to be an unnecessary redundancy and outside the scope of Gennaro.

The section of Gennaro relied upon in rejecting claim 2 discusses the provision of key generating keys to key recovery agents. See col. 9, line 16-17. Gennaro explicitly indicates that each key is generated using only a single set of key generating values. See col. 9, line 6-8. Even if one were to consider the key generating keys to be values by which a key is

determinable (which applicant does not concede), there is no second set of key generating keys in Gennaro by which Gennaro's key is determinable. Rather, there is only a single key generating key from which Gennaro's key is created. Accordingly, applicant submits that claim 2 is independently allowable over Gennaro on this ground.

Claim 10

Claim 10 was rejected under 35 U.S.C. § 102(b) as anticipated by Gennaro.

As amended, claim 10 relates to a method that includes storing, on a server accessible through a network, secured information and a first access component, excluding both the key and the second access component from storage on the server, and providing the secured information and the first access component to a first requestor. Access to the secured information requires a key. The key is determinable using the first access component, a second access component, and a relationship between the first and second access components.

Gennaro neither describes nor suggests storing secured information and a first access component on a server while excluding a key and a second access component from storage on the server, where access to the secured information requires the key and the key is determinable using the first access component, a second access component, and a relationship between the first and second access components.

In Gennaro's system, the entire key to an encrypted message is attached (in encrypted form) to the message itself. When Gennaro's messages are received, they are presumably stored, at least initially, with the message. Such storage of the keys means that the keys are not excluded from storage on the same

server as the secured message information, as recited by claim 10.

Since Gennaro neither describes nor suggests elements and limitations from claim 10, claim 10 is not anticipated by Gennaro. Accordingly, applicant requests that claim 10, and the claims dependent therefrom, be allowed.

Claims 12-15 recite third and fourth access components that also permit access to the secured information. There is nothing in Gennaro that describes or suggests additional access components by which the key to Gennaro's encrypted messages is determinable. Rather, in the context of transmitting a message between a sender and a recipient, additional access components that also permit access to Gennaro's messages would seem to be an unnecessary redundancy and outside the scope of Gennaro.

The rejection of claim 12 relies upon U.S. Patent No. 6,662,299 to Price, III (hereinafter "Price") as showing additional access components. However, these additional access components are split from the *same single key*. See Price, col. 5, line 7-9. Thus, if one were to consider Price's multiple shares as third and fourth access components within the meaning of claim 12, then access to the secured information would not be available solely through the first and second access components (and the relationship therebetween), as required by parent claim 10. Accordingly, applicant submits that claim 12 is independently allowable over Gennaro on this ground.

Claim 18

Claim 18 was rejected under 35 U.S.C. § 102(b) as anticipated by Gennaro.

As amended, claim 18 relates to a method that includes receiving, from a client, a first access component, receiving, from a server accessible through a network, secured information,

and receiving, from a source other than the client or the server, the second access component. Access to the secured information requires a key. The key is determinable using the first access component and a second access component.

Gennaro neither describes nor suggests receiving secured information from a server, receiving a first access component from a client, and receiving a second access component from a source other than the client or the server. As discussed above, Gennaro's messages are sent with attached, but encrypted, keys. As such, the entire keys are received from the same source as the messages and cannot constitute a first or second access component within the meaning of claim 18.

The rejection of former claim 20 contends that the written description of FIG. 9 of Gennaro describes the receipt of a second access component from a source other than the client or the server.

Applicant respectfully disagrees. FIG. 9 of Gennaro describes the first phase of Gennaro's communication system, before encrypted communication sessions occur. See col. 17, line 4-5. In this first phase, a first party (denoted in Gennaro as "Alice") sends a second party (denoted as "Bob") encrypted key generating values KG. See col. 17, line 32-34. The key generating values KG have been encrypted using the public keys of 3rd party agents. See col. 17, line 30-31.

Please note that the key generating values KG cannot constitute an access component within the meaning of claim 18. Although the key generating values KG are used to generate the key generating KH values and the session-specific keys KK, no "second access component" by which the key is determinable is received from a source other than the client or the server. The reconstruction of keys in Gennaro (using key generating values KG or otherwise) requires the private keys of the 3rd party

agents. These private keys are maintained in secrecy by the 3rd party agents, even after the contents of an encrypted communication are recovered. See, e.g., col. 18, lines 31-47.

Since the private keys of the 3rd party agents are never disclosed by the 3rd party agents, they are never received from any source whatsoever and cannot constitute a second access component within the meaning of claim 18.

Accordingly, applicant requests that claim 18, and the claims dependent therefrom, be allowed.

Claim 23

Claim 23 was rejected under 35 U.S.C. § 102(b) as anticipated by Gennaro.

As amended, claim 23 relates to an article comprising a machine-readable medium that stores machine-executable instructions. The instructions are operable to cause a machine to define a key and a set of values, send a first but not all of the set and information encrypted using the key to a server for storage, and send a second but not all of the values of the set to a first delegate. The key is determinable by the values and a predefined relationship between the values. The encrypted information is accessible with the key, inaccessible with the first of the values absent the second of the values, and inaccessible with the second of the values absent the first of the values.

Gennaro neither describes nor suggests instructions that are operable to cause a machine to send a first but not all of the values of a set of values by which the key is determinable and information encrypted using the key to a server for storage. Gennaro also fails to describe or suggest sending a second but not all of the values of the set to a first delegate.

Rather, in Gennaro, the entire key is sent with every message, albeit in encrypted form. There are no separate values by which the key is determinable that are sent with the message.

Even if one were to neglect the fact that Gennaro attaches the entire key to every encrypted message and consider the key to be a first value by which the key is determinable (which applicant does not concede), claim 23 is still not anticipated by Gennaro. In particular, under this interpretation of the claim language, the 3rd parties' private keys (which decrypt the attached key) would be required to be considered values by which the key is determinable. The 3rd parties in Gennaro never transmit their private keys. Rather, they maintain the private keys in secrecy, even after the contents of an encrypted communication are recovered. See, e.g., col. 18, lines 31-47. Therefore, Gennaro neither describes nor suggests instructions that are operable to cause a machine to send a second but not all of the values of the set of values to a first delegate.

Since Gennaro neither describes nor suggests elements and limitations from claim 23, claim 23 is not anticipated by Gennaro. Accordingly, applicant requests that claim 23, and the claims dependent therefrom, be allowed.

Claim 24 recites a second set of values by which a key is determinable. Gennaro describes the transmission of an encrypted message between a sender and a recipient. There is nothing in Gennaro that describes or suggests a second set of values by which the key to Gennaro's encrypted messages is determinable. Rather, in the context of transmitting a message between a sender and a recipient, multiple sets of such values would seem to be an unnecessary redundancy and outside the scope of Gennaro.

The section of Gennaro relied upon in rejecting claim 24 discusses the provision of key generating keys to key recovery

agents. See col. 9, line 16-17. Gennaro explicitly indicates that each key is generated using only a single set of key generating values. See col. 9, line 6-8. Even if one were to consider the key generating keys to be values by which a key is determinable (which applicant does not concede), there is no second set of key generating keys in Gennaro by which Gennaro's key is determinable. Rather, there is only a single key generating key from which Gennaro's key is created. Accordingly, applicant submits that claim 2 is independently allowable over Gennaro on this ground.

Claim 25

Claim 25 was rejected under 35 U.S.C. § 102(b) as anticipated by Gennaro.

As amended, claim 25 relates to an apparatus that includes a processor and instructions configured to cause the processor to receive, from a client, information and a value of a set of values, store the information and the value, but not all the values of the set, and transmit, to a delegate, the information and the value. The information received from the client is encrypted using a key. The key is determinable by the values of the set and a predefined relationship between the values.

Gennaro neither describes nor suggests instructions configured to cause a processor to receive encrypted information and a value of a set of values by which a key that encrypts the information is determinable. Further, Gennaro neither describes nor suggests instructions configured to cause a processor to store encrypted information and a value, but not all the values of a set by which the key to the encrypted information is determinable.

In Gennaro's system, the key to an encrypted message is received along with the encrypted message, rather than a value

by which the key is determinable. Further, when messages are received by Gennaro's system, they are presumably stored, at least initially, with the message. Since the key in Gennaro is treated as a unitary whole, Gennaro neither describes nor suggests not storing all the values of a set by which the key is determinable.

Since Gennaro neither describes nor suggests elements and limitations from claim 25, claim 25 is not anticipated by Gennaro. Accordingly, applicant requests that claim 25, and the claims dependent therefrom, be allowed.

Claim 26 recites a second set of values that are sufficient to determine the key. Gennaro describes the transmission of an encrypted message between a sender and a recipient. There is nothing in Gennaro that describes or suggests a second set of values by which the key to Gennaro's encrypted messages is determinable. Rather, in the context of transmitting a message between a sender and a recipient, multiple sets of such values would seem to be an unnecessary redundancy and outside the scope of Gennaro.

The first section of Gennaro relied upon in rejecting claim 26 describes that multiple key encrypting keys can be used to encrypt a message key. See col. 5, line 66 - col. 6, line 4.

If one were to consider Gennaro's additional key encrypting keys to be a second set of values that are sufficient to determine the key within the meaning of claim 26, then the key would not be determinable solely through the values of the set (and the relationship therebetween) recited in parent claim 26. Accordingly, applicant submits that Gennaro's multiple key encrypting keys cannot constitute a second set of values by which the key to Gennaro's encrypted messages is determinable.

The second section of Gennaro relied upon in rejecting claim 26 discusses the provision of key generating keys to key

recovery agents. See col. 9, line 16-17. Gennaro explicitly indicates that each key is generated using only a single set of key generating values. See col. 9, line 6-8. Even if one were to consider the key generating keys to be values by which a key is determinable (which applicant does not concede), there is no second set of key generating keys in Gennaro by which Gennaro's key is determinable. Rather, there is only a single key generating key from which Gennaro's key is created. Accordingly, applicant submits that claim 26 is independently allowable over Gennaro on this ground.

Claim 29

Claim 29 was rejected under 35 U.S.C. § 102(b) as anticipated by Gennaro.

Claim 29 relates to a method that includes encrypting information using an encryption key, sending the encryption key, but not the encrypted information to a first party, sending the encrypted information, but not the encryption key to a server.

Gennaro neither describes nor suggests sending an encryption key, but not the encrypted information to a first party.

In Gennaro's system, the encryption key is attached, albeit in encrypted form, to the message that it encrypts. Thus, the encrypted information is always sent with the encryption key in the same message.

Further, even if one considers the attached, encrypted key to be "encrypted information," claim 29 is still not anticipated by Gennaro. The encryption key for the attached key are the private keys of Gennaro's 3rd party agents. The 3rd parties in Gennaro never transmit their private keys but rather maintain the private keys in secrecy, even after the contents of an encrypted communication are recovered. See, e.g., col. 18,

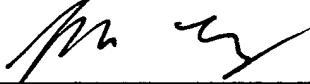
lines 31-47. Thus, the 3rd parties send their private encryption key at all, with or without the encrypted information.

Since Gennaro neither describes nor suggests elements and limitations from claim 29, claim 29 is not anticipated by Gennaro. Accordingly, applicant requests that claim 29, and the claims dependent therefrom, be allowed.

Applicant asks that all claims be allowed. No fees are believed due at this time. Please apply any charges or credits to Deposit Account No. 06-1050.

Respectfully submitted,

Date: 2/7/05



Scott C. Harris
Reg. No. 32,030

By
JOHN F. CONROY
REG # 45,485

Fish & Richardson P.C.
PTO Customer Number: 20985
12390 El Camino Real
San Diego, CA 92130
Telephone: (858) 678-5070
Facsimile: (858) 678-5099
10456179.doc